# HEAL THYSELF

## 5 WAYS HEALTHCARE CAN BEAT PHISHING

Cofense™ works with healthcare customers, among many others, to detect and stop phishing attacks. Here are five tips for building a stronger defense, based on our industry experience and the data we've compiled.

## 1. START BY ACCEPTING REALITY: HEALTHCARE IS A BIG FAT TARGET

### Over 18M Employees/Phishing Targets

Healthcare employs more people than any other industry. They are portals to email addresses, Social Security numbers, credit card numbers, and other information phishing attackers steal for profit. No wonder the healthcare industry has a bullseye on its back.

Source: The Atlantic Monthly, 2018.

### Top 3 Breaches in Healthcare, 2019 to Date

- AMCA — *25M Patients*
- Dominion National — *2.96M Patients*
- Immediata Health Group — *1.5M Patients*

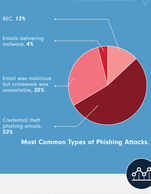
Phishing attacks, along with third-party vendors, were to blame for these attacks.

Health IT Security, July 23, 2019

### $408 to Replace a Stolen Record

That's the industry average vs. $148 across major industries.

Source: Healthcare-Informatics.com, 2018




**Most Common Types of Phishing Attacks.**

### Over 50% of healthcare phishing seeks to steal credentials.

Source: Cofense Phishing Defense Center™

### Over 1 in 10 are Business Email Compromise.

Source: Cofense Phishing Defense Center

## 2. BENCHMARK YOUR PHISHING RESILIENCY. UM, WHAT'S THAT?

### Phishing Resiliency = User Susceptibility: User Reporting

It's the ratio of people who fall susceptible to a phishing email vs. those who report them to security teams. How do you track resiliency? Cofense pioneered phishing simulations over a decade ago. When you send simulated phish to employees' inboxes, you can easily measure how resilient your company is to attacks. A 1:1 ratio is an ok start, but anything over 2:1 shows solid resiliency.

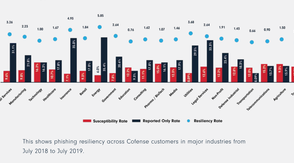

### Healthcare Still Lags Behind!

The chart at left shows how Cofense healthcare customers performed in phishing simulations from July 2018 to July 2019.

### 24% Less Resilient

than other major industries. Healthcare's rate of 1.67 is significantly lower than the cross-industries average of 2.20.

### Energy, Insurance, and Utilities Set the Bar




This shows phishing resiliency across Cofense customers in major industries from July 2018 to July 2019.

## 3. EDUCATE YOUR PEEPS TO REPORT PHISHING EMAILS.

### It works. So far in 2019, resiliency has grown 18.5%.

From January 2019 to July 2019, phishing resiliency among Cofense healthcare customers is tracking at 1.78—nearly 2 employees reporting a simulated phish to every 1 that falls susceptible. That's up from 1.67, a rise of 18.5%.

### Resiliency is solid or (better) against some of the most common attacks

In each of the phishing scenarios below, Cofense healthcare customers achieved a resiliency rate of 2.0 or better.

### Phishing Scenario Resiliency Rate

| Undelivered Messages | Account Security Alert | Order Confirmation | Password Survey | Reset Password |
|---|---|---|---|---|
| 11.77 | 3.99 | 2.85 | 2.33 | 2.26 |

## 4. WORK ACROSS TEAMS TO BUILD RELEVANT DEFENSES.

Security awareness teams that run phishing simulations need input from their colleagues in security operations and threat intelligence. By knowing the attacks your company sees, plus emerging campaigns in the wild, your awareness program can deliver relevant simulations.

### 2 Real Phish That Grabbed Our Attention

The Cofense Phishing Defense Center identifies phishing attacks that are live in customers' environments—campaigns that evaded secure email gateways. Here are three our experts are seeing across top industries, including healthcare.

### Zombie Phish

Using a compromised email account, the attacker sends an email that revives a dead conversation. The email typically contains a malicious link.

### File Sharing Attacks

Cloud-based services like Dropbox and Google Docs are more popular than ever, which makes them a phishing target. When phishing links are embedded in documents from trusted sources, automated defenses sometimes fail to detect them.

## 5. RALLY YOUR HUMAN DEFENDERS

### 10 Minutes to Stop an Attack

One Cofense healthcare customer stopped a credential phish, from start to finish, in just 10 minutes. This company has united its people, both general users and security professionals, in the fight against phishing emails.

### 3 Ways They Did It


**1. Educated employees to recognize phishing -** Within minutes after the phishing campaign launched, numerous employees noticed something suspicious.

**2. Conditioned employees to report -** Employees who saw something said something: they reported the phish with a single click. Enough reports came in to signal trouble.

**3. Gave security teams actionable intelligence -** This company relies on the Cofense Phishing Defense Center to turn user-reported emails into usable intelligence. Within minutes after the phishing campaign started, the company had what it needed to shut down the attack.

To learn more, visit cofense.com/phishing-defense-solutions-healthcare/

COFENSE